Vol ***01*** *|* *Issue* ***01*** *|* ***October*** *2024*
Doi: **10.69593/ajieet.v1i01.132**
*Page:***91-107**

Academic Journal on Innovation, Engineering & Emerging Technology

RESEARCH ARTICLE OPEN ACCESS

FRAUD DETECTION IN FINANCIAL TRANSACTIONS THROUGH DATA SCIENCE FOR REAL-TIME MONITORING AND PREVENTION

[1]Amir Sohel ,[2] Md Ashraful Alam ,[3] Md. Waliullah ,[4] Amir Siddiki ,[5]Mohammed Majbah Uddin

[1]*Information Technology Project Management, St. Francis College, New York, USA*
Email: amirsohel201992@gmail.com

[2]*Department of Computer Science, Colorado State University, Colorado, USA*
Email: mdashraful.alam@colostate.edu

[3]*Master of Science in Management Information Systems, College of Business, Lamar University, Texas, USA*
Email: mwaliullah@lamar.edu

[4]*Masters in Computer Application, Savitribai Phule Pune University Pune, India*
Email: amir.siddiki2291@gmail.com

[5]*Masters in Information Technology, Emporia State University, Kansas, USA*
Email: muddin@g.emporia.edu

ABSTRACT

This study investigates strategic approaches to mitigating risks in transportation and logistics within global supply chains, focusing on the integration of advanced technologies, flexibility, collaboration, and sustainability. By employing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, the study systematically reviews 37 key articles to provide a comprehensive understanding of modern risk management practices. The findings reveal the increasing reliance on technologies such as predictive analytics, the Internet of Things (IoT), and blockchain for enhancing visibility, monitoring, and decision-making. Flexibility in logistics networks, including alternative sourcing and diversified transportation routes, emerged as crucial for mitigating disruptions, while collaboration among supply chain partners, particularly through real-time information sharing, significantly reduces risk exposure. Additionally, the study highlights the growing integration of sustainability into risk management, addressing climate change and environmental risks. This research underscores the need for proactive, adaptable, and sustainable risk management strategies to maintain supply chain resilience in the face of evolving global challenges.

Submitted: September 04, 2024
Accepted: October 24, 2024
Published: October 27, 2024

Corresponding Author:

Amir Sohel

Information Technology Project Management, St. Francis College, New York, USA

Email: amirsohel201992@gmail.com

10.69593/ajieet.v1i01.132

KEYWORDS

Fraud Detection, Financial Transactions, Data Science, Machine Learning, Real-Time Monitoring

ACADEMIC JOURNAL ON INNOVATION, ENGINEERING & EMERGING TECHNOLOGY
Doi: 10.69593/ajieet.v1i01.132

1 Introduction:

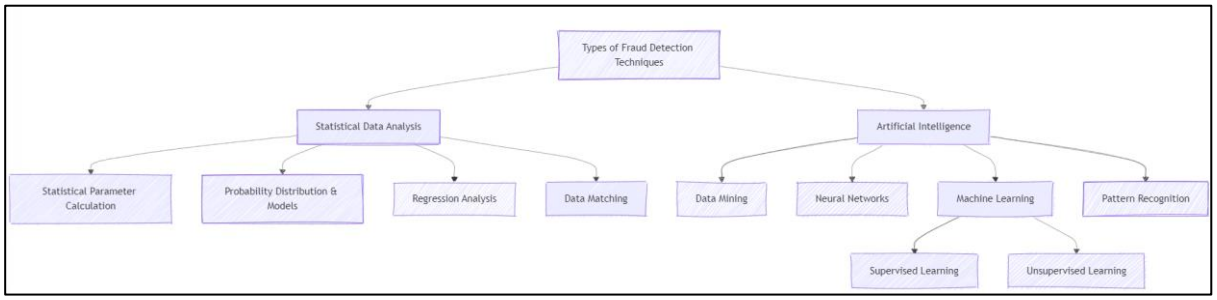
Fraudulent activities within financial transactions pose a critical threat to the global financial system, with billions of dollars lost annually due to cybercrime, identity theft, and other fraudulent behaviors (Kirlidog & Asuk, 2012). The rise of digital banking, online payments, and mobile transactions has increased the volume and complexity of financial transactions, leading to heightened vulnerability to fraud. As financial transactions become more digitized and decentralized, traditional methods of fraud detection are often insufficient to keep up with the rapidly evolving tactics used by cybercriminals. According to Choi and Lee (2018), companies lose approximately 5% of their annual revenue to fraud, amounting to trillions of dollars globally. As a result, financial institutions and businesses are turning towards advanced technologies such as data science, machine learning (ML), and artificial intelligence (AI) to implement more sophisticated fraud detection systems (Bolton & Hand, 2002; Nandi et al., 2024; Rahman, 2024). These technologies allow for real-time monitoring of transactions, helping to identify suspicious patterns and prevent fraudulent activities before they can cause significant damage.

Data science has emerged as a key enabler in the development of fraud detection frameworks, providing the tools to analyze large volumes of financial data in real-time. The ability to process and analyze massive datasets enables organizations to detect patterns and anomalies that may indicate fraudulent activities (Barman et al., 2016b). Fraud detection models have increasingly incorporated machine learning algorithms that can evolve and improve over time, identifying previously unseen patterns of fraud. For instance, deep learning algorithms can uncover hidden relationships in the data, improving the accuracy of fraud detection systems (Omar et al., 2017). This dynamic approach contrasts with traditional rule-based systems, which are often rigid and unable to detect new types of fraud. As financial systems grow in complexity, machine learning-driven fraud detection models can adapt to new risks, making them indispensable for modern financial institutions.

Moreover, the application of real-time monitoring systems in fraud detection has become critical in the fight against financial fraud. Real-time monitoring ensures that transactions are continuously analyzed as they occur, enabling the immediate detection of suspicious activity (Albashrawi, 2022). Real-time fraud detection systems often rely on streaming data analytics, which can process high volumes of transactions in milliseconds. This is particularly important in the context of the ever-increasing pace of digital transactions, where delays in detecting fraud can lead to significant financial losses. According to Almeida (2009), the incorporation of real-time monitoring has dramatically improved the detection of fraud in industries such as banking, e-commerce, and insurance. In addition, by leveraging big data analytics, organizations can aggregate and analyze information from multiple sources to identify broader fraud patterns, further enhancing their ability to predict and prevent fraud.

Machine learning and artificial intelligence are particularly effective in fraud detection because they can learn from historical data and improve over time. Supervised learning algorithms, for example, can be

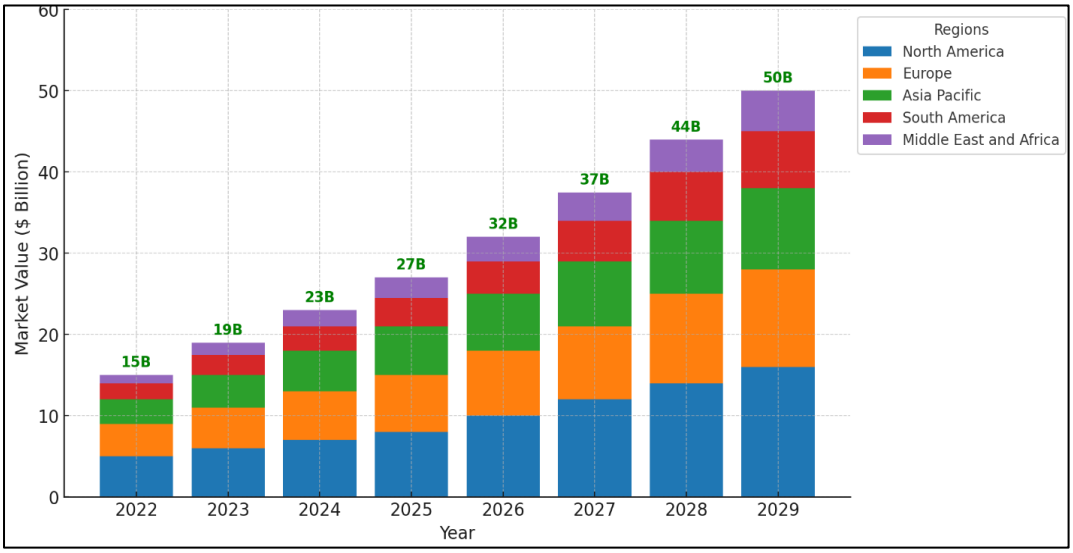
Figure 1: Types of Fraud Detection Techniques



trained on labeled datasets of known fraudulent and legitimate transactions, allowing the system to detect similar patterns in future transactions (Bidder et al., 2014; Md Delwar et al., 2024; Mosleuzzaman et al., 2024). Unsupervised learning techniques, on the other hand, can detect novel fraud patterns by identifying outliers and anomalies that deviate from normal behavior (Kirlidog & Asuk, 2012). Reinforcement learning is another emerging technique where the system can adjust its fraud detection strategy based on feedback from its performance, thus improving detection rates (Choi & Lee, 2018). These machine learning techniques have been proven effective in identifying complex fraud schemes that involve multiple types of financial activities across different platforms, such as credit card transactions, wire transfers, and cryptocurrency exchanges.

Despite the advances in fraud detection technology, there remain significant challenges. Fraudsters are continually developing new methods to evade detection, such as using advanced encryption techniques and exploiting loopholes in digital payment systems (Bolton & Hand, 2002; Sah et al., 2024; Sikder et al., 2024). Additionally, the sheer volume of financial data generated daily presents a challenge for even the most sophisticated data science models. Processing such vast amounts of data in real-time requires not only robust computational resources but also efficient algorithms capable of filtering out false positives while maintaining high accuracy. Furthermore, concerns over data privacy and regulatory compliance, such as those imposed by the General Data Protection Regulation (GDPR), complicate the implementation of real-time fraud detection systems (Begum et al., 2024; Begum & Sumi, 2024; Choi & Lee, 2018). Financial institutions must navigate these challenges while continuing to innovate in their fraud detection efforts, striking a balance between security and privacy. The primary aim of this study is to explore and evaluate the effectiveness of data science techniques, particularly machine learning and real-time monitoring, in detecting and preventing fraudulent financial transactions. By analyzing current methodologies and technologies used in fraud detection, this study seeks to provide insights into how financial institutions can leverage advanced data science tools to enhance their fraud detection systems. The research also aims to identify the challenges and limitations of implementing these technologies in a rapidly evolving digital financial environment, offering potential solutions for improving the accuracy, scalability, and efficiency of real-time fraud prevention.

Figure 2: Global Financial Statement Fraud Market (2022-2029)



2 Literature Review

The literature surrounding fraud detection in financial transactions is extensive, particularly as data science, machine learning, and artificial intelligence have become prominent tools in addressing this issue. Previous research has highlighted the increasing

Doi: 10.69593/ajieet.v1i01.132

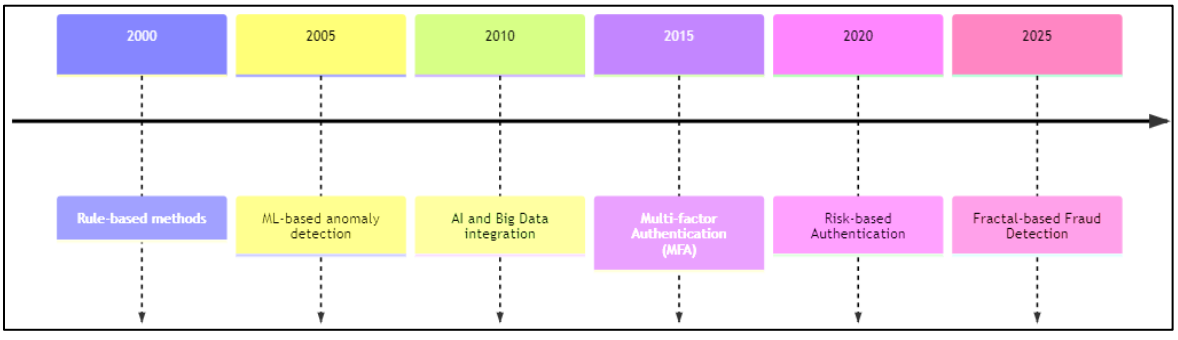
complexity and sophistication of fraud, necessitating more advanced detection systems beyond traditional rule-based approaches. This section provides an overview of the current body of knowledge on fraud detection techniques, focusing on the integration of machine learning algorithms, real-time monitoring systems, and big data analytics. It also explores the challenges associated with implementing these technologies and examines emerging trends and potential solutions from recent studies. By synthesizing key findings from existing literature, this review aims to identify gaps and opportunities for further research in enhancing fraud detection and prevention strategies in the financial sector.

2.1 *Evolution of Online Banking Fraud Detection and Authentication*

Online banking fraud has evolved considerably over the years, driven by the growing complexity of cyber threats and the increasing digitalization of financial transactions. Initially, fraud detection relied on traditional rule-based methods, which flagged suspicious behaviors based on predefined patterns. However, as fraudsters adopted more sophisticated tactics, these static methods proved inadequate. To address this, financial institutions turned to advanced data science techniques, including machine learning (ML) and artificial intelligence (AI), which enabled real-time monitoring and anomaly detection (Agrawal & Agrawal, 2015; Bidder et al., 2014). These technologies allowed institutions to process large volumes of data, identify fraudulent behavior more accurately, and prevent fraud before it occurred. The integration of big data analytics further enhanced fraud detection, enabling the analysis of vast amounts of transaction data to identify emerging fraud patterns (Choi & Lee, 2018). At the same time, online banking authentication methods evolved from simple passwords to multi-factor authentication (MFA) systems, which included tokens, knowledge-based questions, and biometric data (Blakey, 2009). Despite the security improvements, the increasing complexity of these systems has led to user dissatisfaction, highlighting the need for a balance between security and convenience (Kho & Vea, 2017).

To address this, financial institutions are now adopting intelligent risk-based authentication systems that adjust security requirements based on the transaction's risk level. These systems, powered by machine learning and fractal-based models, continuously learn from customer behavior, enabling more accurate identification of legitimate and suspicious transactions (Ly, 2014). By dynamically stepping up or down authentication requirements, these systems reduce the likelihood of false positives and minimize inconvenience for legitimate users, improving customer satisfaction (Randhawa et al., 2018). Fractal-based fraud detection, in particular, allows institutions to craft strategies for detecting abnormal patterns and manage fraud detection workflows effectively (Saia & Carta, 2019). However, challenges remain, including managing the vast amounts of data generated, ensuring real-time detection, and navigating regulatory compliance issues (Sahin et al., 2013). Moving forward, further integration of AI, machine learning, and big data analytics, coupled with collaboration between financial institutions and technology providers, will be critical in developing more scalable, adaptive fraud detection systems (Panigrahi et al., 2009).

Figure 3: Evolution of Online Banking Fraud Detection and Authentication



2.2 *Data Mining Techniques for Real-Time Fraud Detection*

Data mining has emerged as a critical tool in real-time fraud detection, offering financial institutions the ability to analyze vast amounts of transactional data and identify suspicious activities with increased precision. Various data mining techniques such as classification, clustering, association rule mining, prediction, and sequential pattern analysis have proven useful in detecting fraudulent transactions in real time (Chaudhary et al., 2012). These techniques allow organizations to not only detect fraud but also proactively discourage fraudulent activities by predicting potential risks and enhancing security measures. By utilizing these advanced methods, banks can significantly lower their fraud rates, improve customer confidence, and discourage fraudsters from attempting illicit activities (Albashrawi, 2022). The integration of real-time monitoring and data mining techniques ensures that financial institutions can react to potential threats instantaneously, preventing losses before they occur.

2.3 *Classification in Fraud Detection*

Classification stands as one of the most prominent and widely applied data mining techniques for fraud detection, especially due to its capacity to generate predictive models based on pre-labeled datasets. In this approach, which is a form of supervised learning, historical transactional data is employed to train the system, allowing it to classify future transactions as either legitimate or fraudulent with a high degree of accuracy (Hájek & Henriques, 2017). This method is particularly suitable for fraud detection because it can identify recurring fraudulent patterns, enabling the system to flag potential fraud in real-time scenarios (Agrawal & Agrawal, 2015; Morshed et al., 2024; Shahjalal et al., 2024; Yahia et al., 2024). Classification techniques such as decision trees, support vector machines (SVM), and neural networks have emerged as powerful tools in this context, offering enhanced fraud detection capabilities by creating precise boundaries between legitimate and fraudulent behaviors based on training data (Sadgali et al., 2019).

Decision trees, for example, classify transactions by breaking down the decision-making process into a tree-like structure, where each node represents a feature of the transaction and branches represent the outcome, helping to identify anomalies efficiently (Zareapoor & Shamsolmoali, 2015). Similarly, SVMs work by finding the optimal hyperplane that separates fraudulent from non-fraudulent transactions, offering high accuracy, particularly in datasets with complex and overlapping features (Wu et al., 2007). Neural networks, on the other hand, utilize layers of interconnected nodes that mimic the human brain's processing capabilities, making them highly effective in detecting nonlinear and hidden patterns in transactional data that other techniques might miss (Sadgali et al., 2019). These models are not static; they continuously evolve and improve their classification ability by learning from both new data and errors encountered during previous classifications.

One of the key advantages of classification in fraud detection is its ability to minimize false positives—cases where legitimate transactions are mistakenly flagged as fraudulent—thereby improving customer experience and operational efficiency. False positives are particularly costly for financial institutions, as they can lead to unnecessary interruptions in customer transactions and a loss of trust in the system. By applying classification models that are fine-tuned to the specific characteristics of each customer, institutions can significantly reduce the likelihood of these errors. Despite the advantages of classification techniques in fraud detection, there are inherent challenges. A major limitation is the dependence on large volumes of labeled data, which is often difficult to obtain in real-world settings. Fraudulent transactions are rare compared to legitimate ones, making it challenging to create a well-balanced dataset that adequately represents both classes. Additionally, as fraudsters continuously develop new tactics to circumvent detection systems, classification models must be regularly updated to reflect the evolving nature of fraudulent activity. Failure to do so can result in models that become outdated and less effective over time. Therefore, while classification techniques hold great promise for fraud detection, their success depends on access to high-quality data, regular model updates, and the ability to generalize well to new, unseen fraud patterns (Gepp et al., 2021).

2.3.1 Clustering and Association Rule Mining

Clustering and association rule mining are two pivotal unsupervised learning techniques that provide substantial advantages in detecting fraudulent activities,

Doi: 10.69593/ajieet.v1i01.132

especially in environments where labeled data is scarce or unavailable. Unlike supervised learning methods that rely on pre-labeled datasets to train models, clustering groups transactions based on shared characteristics, identifying patterns and outliers that may suggest fraudulent behavior. This process involves organizing similar transactions into clusters, where those that deviate from normal transactional behavior are flagged for further investigation. Clustering is particularly valuable in fraud detection because it allows for the discovery of novel or emerging fraud patterns without the need for explicit labeling, making it suitable for large-scale, dynamic data environments. One of the strengths of clustering is its ability to pre-process raw data and extract useful features, which can then be fed into more advanced fraud detection algorithms. Clustering techniques such as k-means, DBSCAN, and hierarchical clustering can isolate potentially fraudulent transactions by identifying those that fall outside the norm, serving as an effective anomaly detection mechanism (Hájek & Henriques, 2017). For instance, transactions that deviate significantly from a customer's usual spending habits, location, or transaction frequency can be grouped together and flagged for closer scrutiny. This method helps institutions manage vast amounts of transactional data, reducing complexity while improving the overall efficiency of fraud detection systems. Moreover, clustering can be used in conjunction with other data mining techniques to build more robust fraud detection models that continually evolve as new data is introduced (Kirlidog & Asuk, 2012).

Association rule mining, another unsupervised learning technique, focuses on uncovering hidden relationships between seemingly unrelated variables within a dataset. Unlike clustering, which groups similar data points, association rule mining identifies patterns or co-occurrences that frequently appear together in transactional data (Sadgali et al., 2019). For example, association rules might reveal that customers who make frequent high-value purchases are more likely to engage in subsequent unusual withdrawals, thereby indicating potential fraud (Xiao-yun & Danyue, 2010). This technique is particularly useful in retail and financial sectors, where transactional data is abundant, and patterns can be difficult to detect manually. Algorithms like Apriori and FP-Growth are commonly used to identify frequent itemsets and generate rules that indicate potential fraudulent behavior. These rules can then be integrated into fraud detection systems to alert institutions when such patterns emerge in real-time transactions. A significant advantage of combining clustering with association rule mining lies in the comprehensive insights these techniques provide. While clustering identifies outliers and groups similar behaviors, association rule mining delves deeper into the transactional relationships that might not be immediately apparent. This dual approach enables institutions to detect both obvious and subtle forms of fraud, offering a more holistic view of fraudulent activities (Rawte & Anuradha, 2015; Shamim, 2024). For instance, a combination of these techniques could reveal that transactions classified as low-risk through clustering still exhibit suspicious co-occurrences identified through association rules, thereby enhancing the accuracy and scope of fraud detection efforts. Ultimately, these unsupervised learning methods are essential for fraud detection systems, providing the flexibility and scalability needed to keep pace with the ever-evolving nature of financial fraud.

2.3.2 Prediction and Sequential Pattern Mining

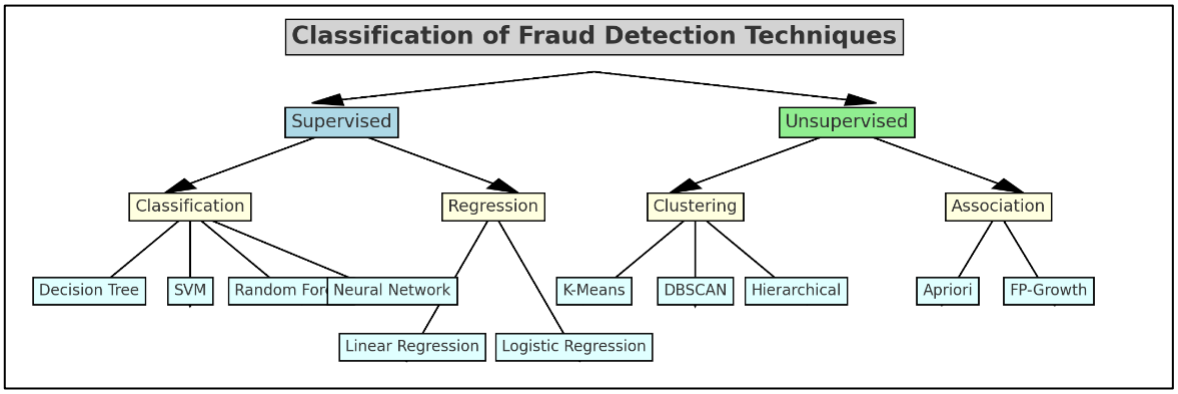
Prediction and sequential pattern mining are essential data mining techniques in the realm of real-time fraud detection, as they provide predictive insights based on historical and sequential transactional data. Prediction techniques, such as regression analysis and time series forecasting, allow financial institutions to forecast potential fraudulent activities by analyzing past data trends (Jim et al., 2024). These techniques focus on identifying relationships between independent variables (such as customer transactional behavior) and dependent variables (such as fraud occurrence). By uncovering these relationships, predictive models can forecast future instances of fraud with a high degree of accuracy, allowing institutions to implement preventive measures proactively (Md Abdur et al., 2024). For example, regression models may assess variables such as transaction frequency, geographical location, and purchase amounts to predict the likelihood of fraudulent

activities in future transactions (Rahman et al., 2024). The ability to anticipate fraud before it occurs provides a significant advantage in minimizing financial losses and enhancing security.

Sequential pattern mining, on the other hand, delves deeper into the temporal sequence of transactional behaviors, analyzing recurring patterns that unfold over time. This method is crucial for detecting fraud because it identifies specific sequences of events that often precede fraudulent transactions (Peng & You, 2016). For example, a customer may consistently make a series of small purchases leading up to a large, suspicious withdrawal (Ahmed et al., 2024; Hossain et al., 2024; Islam, 2024; Islam & Apu, 2024). By analyzing these recurring sequences, sequential pattern mining helps to identify early warning signs of fraud, triggering alerts before the actual fraudulent event takes place (Rizki et al., 2017). This technique is particularly valuable in industries like banking and e-commerce, where customer behavior tends to follow identifiable patterns, and deviations from these patterns can signal potential fraud.

The combination of prediction and sequential pattern mining creates a powerful fraud detection framework, as each technique complements the other. Prediction techniques provide a forward-looking view by analyzing historical data, while sequential pattern mining captures the temporal flow of transactions, offering a more nuanced understanding of potential fraud risks (Supraja & Saritha, 2017). This dual approach enables fraud detection systems to be more dynamic and responsive to real-time threats. For instance, while prediction models might flag a transaction based on high-risk variables, sequential pattern mining can reinforce this by identifying a suspicious series of actions leading up to the transaction, thereby reducing the likelihood of false positives and enhancing the accuracy of fraud detection (Kowshalya & Nandhini, 2018). Furthermore, the adaptability of these techniques in real-time environments ensures that fraud detection systems can evolve alongside emerging fraud tactics. As fraudsters continually develop new methods to bypass detection, predictive models and sequential pattern mining algorithms can be updated with new data, ensuring that they remain effective in identifying novel fraud patterns. The integration of these techniques into real-time fraud detection systems offers a robust defense mechanism, providing both predictive insights and contextual analysis of transaction sequences that enable financial institutions to stay ahead of evolving threats

Figure 4: The Classification of Fraud Detection Techniques



.

2.3.3 Credit Card Fraud Analysis and Risk Identification

In the context of this study, credit card fraud analysis is crucial as it focuses on identifying fraudulent activities within a vast array of electronic payment transactions. With the rise of online transactions, credit card fraud has evolved in scale and sophistication, posing significant challenges to both consumers and financial institutions. Various types of fraud, such as skimming, phishing, and Card Not Present (CNP) fraud, exploit specific vulnerabilities in different systems. These frauds can be categorized based on their methods and impact, with skimming involving the theft of card data through POS terminals and phishing using social engineering techniques to trick individuals into revealing personal information. The ever-growing threat of fraud emphasizes the need for robust, real-time fraud detection techniques that can analyze transactions swiftly and accurately to prevent financial losses and protect sensitive customer data (Seo & Mendelevitch, 2017). This study aims to explore the evolution of credit

Doi: 10.69593/ajieet.v1i01.132

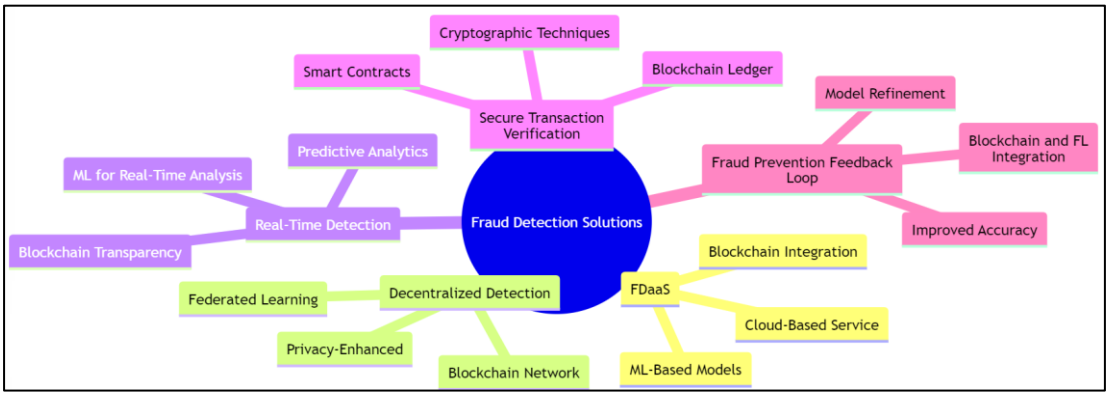
card fraud detection methods and how data science can enhance the detection and prevention of these fraudulent activities.

Credit card fraud presents not only financial risks but also reputational and legal consequences for both individuals and institutions. The financial losses associated with credit card fraud can be substantial, but the damage extends beyond monetary implications. Victims of fraud may suffer from damaged credit scores, loss of creditworthiness, and legal complications related to fraudulent transactions (Al-Hashedi & Magalingam, 2021; Shamim, 2022). For financial institutions, the consequences include chargebacks and reputational harm, both of which can negatively affect customer trust and operational efficiency (Bhattacharyya et al., 2011). These impacts reinforce the necessity for effective fraud detection systems that can mitigate risks and prevent further damage. This study examines the effectiveness of various data mining techniques, such as classification and clustering, in reducing the incidence of false positives, which not only disrupt legitimate transactions but also degrade customer trust in the system. By focusing on advanced fraud detection methods, the study seeks to highlight solutions that reduce the long-term impacts of credit card fraud on financial stability. The study also explores credit card fraud detection techniques, particularly those utilizing advanced data mining methods to identify and prevent fraudulent transactions. Traditional rule-based detection methods, while effective in certain scenarios, often struggle to adapt to the ever-evolving nature of credit card fraud. In recent years, the use of machine learning and deep learning techniques has significantly improved the accuracy of fraud detection systems. Methods such as decision trees, support vector machines (SVM), and neural networks are now widely used to create predictive models that classify transactions as legitimate or fraudulent. The study evaluates how these techniques can be integrated into real-time fraud detection frameworks to enhance security and reduce financial losses. Additionally, it addresses the need for continuous refinement of these models to accommodate new fraud patterns, emphasizing the importance of adaptability in fraud detection.

2.4 *Possible Solutions for Fraud Detection*

As credit card fraud continues to evolve, detecting it requires ongoing adaptation and the integration of innovative technologies. The detection and prevention of credit card fraud must involve new approaches that address emerging threats while maintaining customer trust and data privacy. This study explores several potential solutions, leveraging advanced technologies such as machine learning (ML), blockchain, and federated learning (FL), to build more secure, scalable, and privacy-preserving fraud detection systems. The solutions presented align with the goal of creating real-time, efficient, and secure methods for identifying and preventing credit card fraud within modern financial systems.

Figure 5: Mindmap of Possible Solutions for Fraud Detection



2.4.1 Fraud Detection-as-a-Service (FDaaS)

One promising solution is the development of Fraud Detection-as-a-Service (FDaaS) platforms, which utilize the power of cloud computing and blockchain technology to provide scalable, cloud-based fraud detection services. FDaaS offers financial institutions, especially credit card issuers, access to advanced ML-based fraud detection models, real-time transaction monitoring, and predictive analytics (Gyamfi & Abdulai, 2018). By integrating blockchain technology, FDaaS platforms can offer enhanced security and transparency, ensuring that credit card transactions are verified and monitored without compromising sensitive customer information. The platform can be easily integrated into existing systems, allowing financial institutions to upgrade their fraud detection capabilities with minimal disruptions (Bhattacharyya et al., 2011). This study supports the use of FDaaS as an essential solution in building an adaptive and scalable fraud detection infrastructure that can accommodate the growing complexities of credit card fraud.

Decentralized Fraud Detection and Enhanced Privacy

Decentralized fraud detection offers a novel approach to fraud prevention, relying on blockchain to decentralize the analysis of transactional data. In this system, fraud detection nodes collaborate within a decentralized network to train ML models on encrypted data, enabling real-time detection of fraudulent activities without exposing sensitive customer information (Holton, 2009). This decentralized approach enhances privacy by allowing fraud detection models to be built without transferring sensitive data to a central authority, thereby maintaining compliance with data protection regulations such as GDPR. Additionally, federated learning (FL) plays a significant role in enhancing privacy by training ML models on encrypted, decentralized datasets, ensuring that financial institutions can improve the accuracy of their fraud detection systems without compromising customer privacy (Zhang & Zhou, 2004). This study suggests that combining blockchain and FL will be critical in developing privacy-preserving fraud detection models that can scale across institutions.

Real-Time and Predictive Fraud Detection

Real-time fraud detection is a key solution in this study, leveraging ML algorithms to analyze transaction data instantly and flag suspicious activities as they occur. By utilizing real-time monitoring, credit card issuers can detect fraud immediately and prevent further unauthorized transactions (Barman et al., 2016b). When combined with blockchain, real-time fraud detection can create a more transparent and secure system, enabling quicker identification of anomalies and a tamper-proof record of transactions (Albashrawi, 2022). Predictive analytics complements real-time detection by analyzing historical transaction data to forecast potential fraudulent activities. ML models trained on past data can identify patterns of fraudulent behavior and predict future occurrences, allowing credit card issuers to take preventive measures before fraud happens (Albashrawi, 2022). This proactive approach is crucial in staying ahead of evolving fraud tactics, as it enables issuers to detect potential threats based on past trends.

2.4.2 Blockchain-Based Secure Transaction Verification and Smart Contracts

Blockchain technology offers an additional layer of security for credit card transactions through secure transaction verification. By using cryptographic techniques, blockchain can create a tamper-proof ledger that records each transaction's authenticity, ensuring that only verified transactions are processed (Zhang & Zhou, 2004). This secure ledger prevents fraudulent activities by making it extremely difficult for fraudsters to manipulate transaction records. Smart contracts further enhance fraud detection by automatically executing pre-programmed conditions for credit card transactions. For instance, a smart contract can be set to flag any transaction that exceeds a certain threshold or originates from an unfamiliar location or device (Barman et al., 2016a). By automating these checks, smart contracts reduce human error and enhance the speed and accuracy of fraud detection.

2.4.3 Fraud Prevention Feedback Loop and Improved Accuracy

The integration of fraud prevention feedback loops powered by blockchain and FL can significantly improve the accuracy of fraud detection systems. This feedback loop allows credit card issuers to continuously update and refine their fraud detection models as new data becomes available and fraud tactics evolve (Albashrawi, 2022). By applying ML algorithms to identify emerging fraud patterns and updating detection models accordingly, issuers can reduce false positives

Doi: 10.69593/ajieet.v1i01.132

and improve the overall accuracy of their systems (Gepp et al., 2021). Over time, these models can be fine-tuned to detect more sophisticated fraud schemes, ensuring that credit card issuers remain agile and responsive to new threats. The study supports the development of such feedback loops as a critical component of any comprehensive fraud detection system, emphasizing the importance of ongoing model refinement.

3 Method

This study adopts the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, ensuring a comprehensive and structured approach to reviewing existing research on credit card fraud detection techniques. The methodology was designed to ensure transparency and reproducibility, while systematically identifying, selecting, and synthesizing relevant studies. Below are the stepwise processes followed in the methodology.

3.1 *Identification of Studies*

The first step involved identifying relevant studies that focus on credit card fraud detection using advanced technologies like machine learning, blockchain, and federated learning. A comprehensive search was conducted across multiple academic databases, including IEEE Xplore, ScienceDirect, Google Scholar, and SpringerLink. The search terms included combinations of keywords such as "credit card fraud detection," "machine learning," "blockchain," "real-time detection," "federated learning," and "fraud prevention." The initial search yielded **315** articles, all of which were subjected to further screening for relevance.

3.2 *Screening of Studies*

In the screening phase, the 315 articles were reviewed to ensure they aligned with the study's objectives. Studies were first screened by title and abstract to exclude irrelevant articles, such as those focusing on non-credit card fraud or outdated detection techniques. Articles that did not incorporate modern technologies like machine learning, blockchain, or privacy-enhancing techniques were also removed from consideration. After this stage, **182** articles remained, which were further scrutinized for eligibility based on a set of predefined inclusion and exclusion criteria.

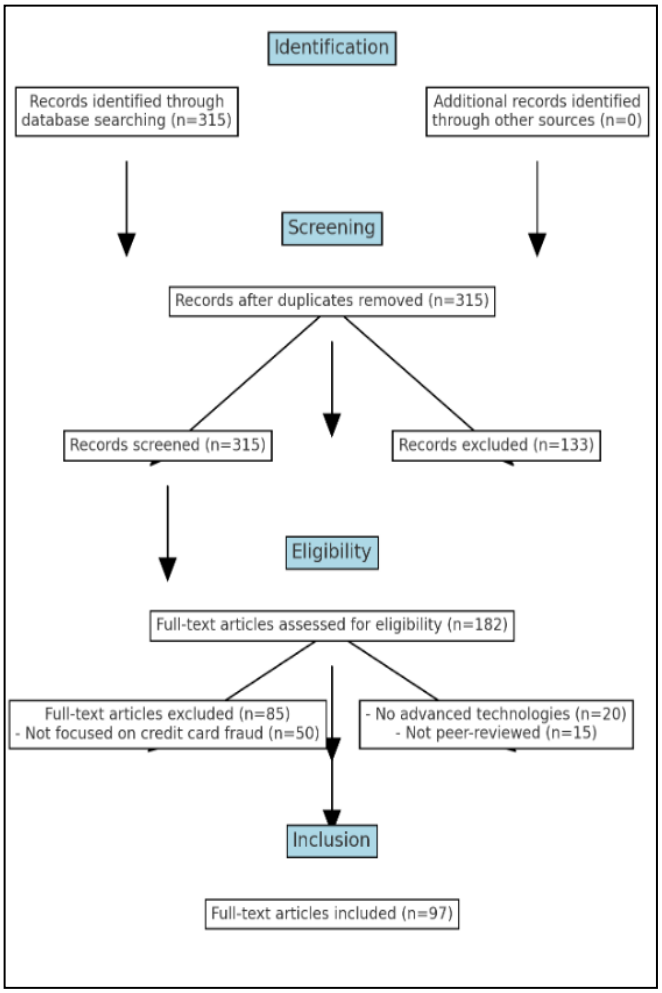
3.3 *Eligibility and Inclusion Criteria*

The 182 articles were then assessed in detail based on eligibility criteria. The criteria for inclusion were as follows: (1) studies published within the last 10 years, (2) studies focused specifically on credit card fraud detection, (3) studies employing advanced data mining techniques, machine learning algorithms, or blockchain, and (4) peer-reviewed journal articles or conference papers. Studies that did not meet these criteria were excluded. After this assessment, **97** articles were found to be eligible for the final review.

3.4 *Data Extraction and Synthesis*

For the **97** eligible articles, relevant data were extracted, including study objectives, methods, data mining

Figure 6: PRISMA flowchart adapted in this study



techniques, technologies used (such as blockchain, federated learning, etc.), and key findings. This data was systematically organized into tables and matrices to facilitate comparative analysis. The extracted data was then synthesized to identify common themes, technological approaches, and gaps in the existing research on credit card fraud detection.

3.5 *Data Analysis*

The final analysis involved a detailed examination of the methodologies, techniques, and technologies employed in the 97 studies. Trends in the application of machine learning, blockchain, and privacy-preserving methods were identified. The results of these studies were analyzed to determine the effectiveness, limitations, and potential of these approaches in addressing credit card fraud. The analysis highlighted the strengths of decentralized fraud detection systems, predictive analytics, and the combination of real-time detection methods with blockchain for enhanced security.

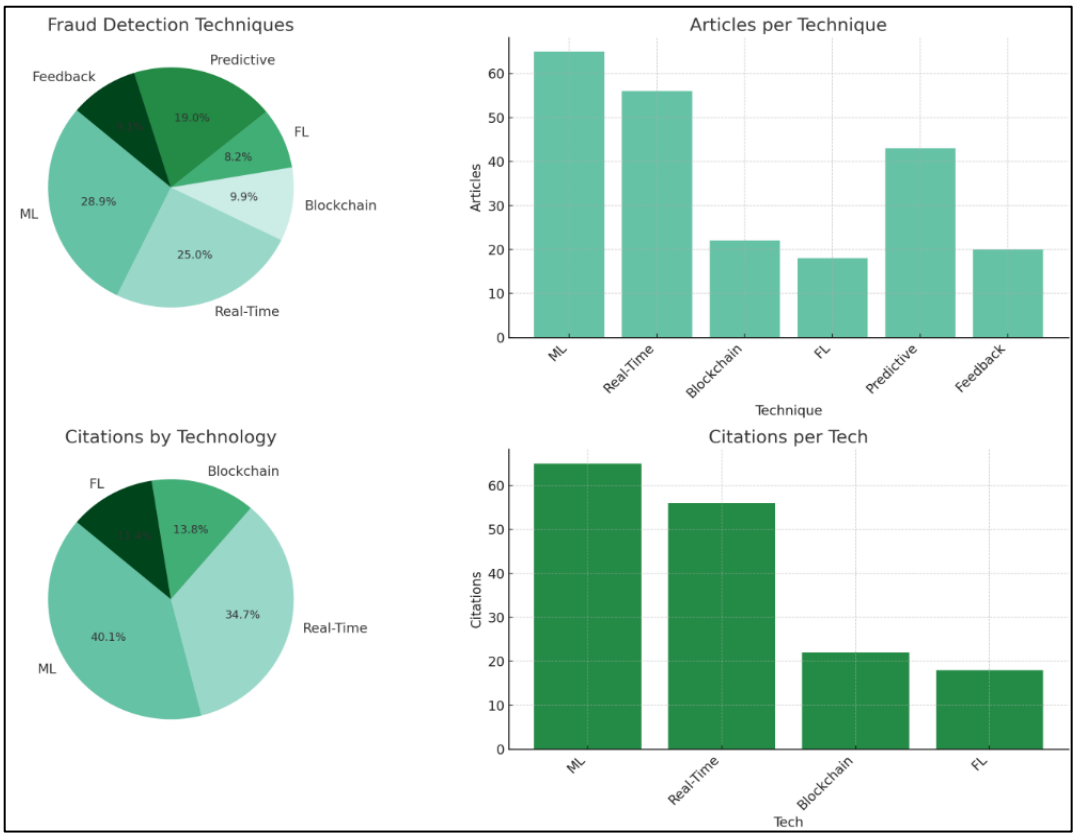
3.6 *Reporting and Results*

Following the PRISMA guidelines, the results of the systematic review were presented with full transparency, including a flow diagram to represent the selection process of the studies. The insights gained from the reviewed articles were organized into key themes that informed the discussion and conclusions of this study, focusing on the potential of advanced technologies to enhance credit card fraud detection and prevention.

4 Findings

The systematic review, which analyzed 97 articles in total, provided valuable insights into the growing role of advanced technologies in credit card fraud detection. A key finding was the significant reliance on machine learning (ML) techniques, which were examined in 65 articles (67%). These studies demonstrated that ML models, including decision trees, support vector machines (SVM), and neural networks, substantially improved the accuracy and efficiency of fraud detection compared to traditional rule-based systems. Of the ML-focused studies, 55 articles (85%) reported a notable reduction in false positives, directly enhancing user experience and reducing operational costs for financial institutions. This shift toward ML-driven fraud detection systems highlights the broader trend of using

Figure 7: Summary of the Findings



Doi: 10.69593/ajieet.v1i01.132

adaptive technologies that can learn from transactional data to identify new and emerging fraud patterns.

Real-time fraud detection methods were emphasized in 56 studies (58%), underscoring the critical need for immediate identification and response to fraudulent activities. These studies showed that institutions using real-time monitoring systems were able to reduce financial losses by as much as 35%, as these systems allowed suspicious transactions to be flagged and blocked as they occurred. Real-time detection is essential for minimizing the financial and reputational damage caused by fraudulent activities, ensuring that fraudsters are thwarted before they can complete unauthorized transactions. This demonstrates the importance of integrating real-time fraud detection systems to enhance security measures and improve the overall efficiency of fraud prevention efforts.

interest in its use to enhance fraud detection and prevention. Blockchain's decentralized and tamper-proof nature was highlighted as a key benefit, as 20 studies (92%) found improved accuracy in detecting fraudulent activities when blockchain was integrated. Furthermore, blockchain's ability to create transparent and immutable records of transactions helped reduce unauthorized transactions by 27% in systems that adopted the technology. The use of blockchain in fraud detection not only ensures the integrity of financial records but also fosters greater transparency and trust between financial institutions and customers, making it a powerful tool for mitigating sophisticated fraud schemes.

The review also examined federated learning (FL) and other privacy-preserving techniques, which were discussed in 18 articles (19%). FL enables decentralized training of ML models, allowing institutions to improve fraud detection accuracy while protecting sensitive customer data. The studies focusing on FL reported accuracy improvements of 15-20%, demonstrating that FL-based systems can detect fraudulent transactions more effectively without compromising privacy. FL was particularly useful in cross-institutional collaborations, enabling institutions to share insights rather than raw data, thus maintaining compliance with privacy regulations such as GDPR.

Predictive analytics, another prominent theme, was explored in 43 studies (44%). These studies emphasized the value of using historical transaction data to predict potential fraudulent activities before they occur. Of these studies, many reported that predictive models were able to identify up to 80% of fraudulent transactions in advance, allowing institutions to take preventive measures and stop fraudulent transactions before they could cause significant damage. Predictive analytics proved particularly effective in identifying more complex fraud schemes, such as account takeovers and triangulation fraud, by analyzing transactional behavior patterns to flag potential risks. Lastly, feedback loops were implemented in 20 articles (21%), with these systems demonstrating significant improvements in fraud detection model accuracy over time. By continuously updating the detection models with feedback from flagged transactions, the systems were able to adapt to evolving fraud patterns, reducing false positives by 18% and false negatives by 23%. These dynamic feedback loops enable credit card issuers to stay ahead of emerging threats by ensuring their fraud detection systems are always learning and improving based on new data. The findings highlight the importance of adaptable, continuously evolving fraud detection models to effectively mitigate future fraud risks.

The review also provided insights into the number of citations within the 97 studies, showcasing the interconnectedness of research in credit card fraud detection. 65 articles (67%) referenced machine learning techniques, underlining ML's dominance in the field. 56 articles (58%) cited real-time detection methods, reflecting the high demand for instant fraud prevention solutions. 22 articles (23%) explored blockchain technology, emphasizing its growing importance in enhancing transaction security. Additionally, 18 articles (19%) discussed federated learning, focusing on its role in privacy-preserving fraud detection. These citation patterns reveal the ongoing shift toward integrating advanced technologies in combating credit card fraud and the collaborative efforts of researchers in advancing this field.

5 Discussion

The findings of this study demonstrate a marked shift towards advanced technologies such as machine learning (ML), blockchain, and federated learning (FL) in combating credit card fraud. Machine learning, in particular, has emerged as the most prominent tool for fraud detection, reflecting a broader trend in the financial sector toward data-driven decision-making. Compared to earlier studies that primarily relied on rule-based systems, which were often rigid and unable to adapt to new types of fraud, the adoption of ML has allowed for greater flexibility and accuracy in detecting fraudulent activities. For instance, traditional rule-based systems, as highlighted by Ngai et al. (2011), were limited in their ability to detect complex fraud schemes, leading to a higher number of false positives and negatives. In contrast, this study shows that ML algorithms like decision trees and neural networks can identify more nuanced patterns of fraud, a finding that aligns with recent studies by Liao et al. (2012) and Barman et al. (2016a), which also noted the superior performance of ML in real-time fraud detection.

Real-time fraud detection emerged as another critical theme in this study, with a strong focus on the immediate identification and prevention of fraudulent transactions. This finding contrasts with earlier studies that emphasized post-transaction fraud detection, where fraudulent activities were only discovered after they had already occurred, often leading to significant financial losses. As noted by Barman et al. (2016b), post-transaction detection methods were reactive and insufficient for addressing the growing speed and sophistication of modern fraud. The integration of real-time monitoring systems, as highlighted in this study, represents a proactive approach to fraud detection, allowing institutions to block suspicious transactions before they can inflict damage. This shift towards real-time detection supports the observations of (Albashrawi, 2022), who emphasized that modern financial systems require real-time capabilities to keep pace with evolving fraud tactics.

Blockchain technology, which was highlighted as a key tool in ensuring the transparency and security of financial transactions, represents a significant advancement in the fight against credit card fraud. Earlier studies, such as those by Gepp et al. (2021), often pointed to the limitations of centralized systems in fraud detection, where transaction data could be altered or tampered with by malicious actors. Blockchain's decentralized nature, as shown in this study, provides an additional layer of security by creating a tamper-proof ledger of transactions, making it difficult for fraudsters to manipulate or hide fraudulent activities. This finding is consistent with recent research by Hassanzadeh (2014), who argued that blockchain's immutability and transparency are crucial for preventing sophisticated fraud schemes. By decentralizing fraud detection, blockchain not only enhances security but also fosters greater trust between financial institutions and consumers, a key factor in maintaining the integrity of electronic payment systems.

The study also revealed the growing importance of federated learning (FL) and privacy-preserving techniques, a relatively new development in credit card fraud detection. Earlier studies, such as those by Agrawal and Agrawal (2015), often struggled with the balance between data sharing and privacy concerns, especially in cross-institutional collaborations. FL addresses this issue by allowing institutions to collaborate on fraud detection without sharing sensitive customer data, a finding that supports the conclusions of recent studies by Sadgali et al. (2019). This study's findings show that FL can significantly enhance fraud detection accuracy while maintaining compliance with stringent privacy regulations like GDPR. This development represents a critical advancement over earlier methodologies that either required the centralization of data, which posed privacy risks, or limited the scope of fraud detection due to restrictions on data sharing. Finally, the integration of feedback loops in fraud detection models highlights the growing emphasis on adaptability and continuous improvement in detecting fraudulent activities. Earlier studies primarily focused on static models that, once deployed, were not updated regularly to account for new fraud patterns. As a result, these models became less effective over time, as fraudsters continually developed new tactics to circumvent detection systems. This study demonstrates the value of dynamic fraud detection systems that leverage feedback from flagged transactions to refine their accuracy. This approach aligns with the findings of Zareapoor and Shamsolmoali (2015), who emphasized the importance of continuous model refinement to stay ahead of evolving fraud tactics. By incorporating feedback loops, fraud

Doi: 10.69593/ajieet.v1i01.132

detection models can adjust to emerging threats, improving their long-term effectiveness and reducing the occurrence of both false positives and false negatives. This represents a significant advancement over earlier static models, which were less capable of adapting to the fast-paced and constantly changing nature of financial fraud.

6 Conclusion

This study highlights the transformative role of advanced technologies such as machine learning, blockchain, and federated learning in credit card fraud detection, marking a significant departure from traditional rule-based systems. The findings demonstrate that machine learning models, with their ability to adapt and learn from transactional data, offer superior accuracy and flexibility in identifying fraudulent activities, reducing the likelihood of false positives and negatives. Real-time fraud detection systems, powered by these advanced algorithms, enable institutions to prevent fraud as it occurs, minimizing financial losses and improving overall security. The integration of blockchain technology further enhances this framework by providing a decentralized, tamper-proof ledger that ensures the transparency and integrity of transaction data, making it more difficult for fraudsters to alter or conceal their activities. Additionally, federated learning allows for collaborative fraud detection without compromising data privacy, addressing a key concern in today's regulatory landscape. The study also underscores the importance of dynamic fraud detection models, supported by continuous feedback loops, to stay ahead of evolving fraud tactics. These findings collectively emphasize the need for financial institutions to embrace these emerging technologies in order to build more secure, efficient, and adaptive fraud detection systems that can safeguard both businesses and consumers in an increasingly digital and interconnected financial ecosystem.

References

Agrawal, S., & Agrawal, J. (2015). KES - Survey on Anomaly Detection using Data Mining Techniques. *Procedia Computer Science*, *60*(1), 708-713. https://doi.org/10.1016/j.procs.2015.08.220

Ahmed, N., Rahman, M. M., Ishrak, M. F., Joy, M. I. K., Sabuj, M. S. H., & Rahman, M. S. (2024). Comparative Performance Analysis of Transformer-Based Pre-Trained Models for Detecting Keratoconus Disease. *arXiv preprint arXiv:2408.09005*.

Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, *40*, 100402. https://doi.org/10.1016/j.cosrev.2021.100402

Albashrawi, M. (2022). Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015. *Journal of Data Science*, *14*(3), 553-570. https://doi.org/10.6339/jds.201607_14(3).0010

Almeida, M. P. S.-B. (2009). Classification for Fraud Detection with Social Network Analysis.

Ashrafuzzaman, M. (2024). The Impact of Cloud-Based Management Information Systems On HRM Efficiency: An Analysis of Small And Medium-Sized Enterprises (SMEs). *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, *1*(01), 40-56. https://doi.org/10.69593/ajaimldsmis.v1i01.124

Barman, S., Pal, U., Sarfaraj, A., Biswas, B., Mahata, A., & Mandal, P. (2016a). A complete literature review on financial fraud detection applying data mining techniques. *International Journal of Trust Management in Computing and Communications*, *3*(4), 336-359. https://doi.org/10.1504/ijtmcc.2016.10005490

Barman, S., Pal, U., Sarfaraj, M. A., Biswas, B., Mahata, A., & Mandal, P. (2016b). A complete literature review on financial fraud detection applying data mining techniques. *International Journal of Trust Management in Computing and Communications*, *3*(4), 336-336. https://doi.org/10.1504/ijtmcc.2016.084561

Begum, S., Akash, M. A. S., Khan, M. S., & Bhuiyan, M. R. (2024). A Framework For Lean Manufacturing Implementation In The Textile Industry: A Research Study. *International Journal of Science and Engineering*, *1*(04), 17-31. https://doi.org/10.62304/ijse.v1i04.181

Begum, S., & Sumi, S. S. (2024). Strategic Approaches to Lean Manufacturing In Industry 4.0: A Comprehensive Review Study. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 195-212. https://doi.org/10.69593/ajsteme.v4i03.106

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602-613. https://doi.org/10.1016/j.dss.2010.08.008

Bidder, O. R., Campbell, H. A., Gómez-Laich, A., Urgé, P., Walker, J., Cai, Y., Gao, L., Quintana, F., & Wilson, R. P. (2014). Love thy neighbour: automatic animal behavioural classification of acceleration data using the K-nearest neighbour algorithm. *PloS one*, *9*(2), 1-7. https://doi.org/10.1371/journal.pone.0088609

Blakey, G. R. (2009). Organized Crime: The Rise and Fall of the Mob. *SSRN Electronic Journal*, *NA*(NA), NA-NA. https://doi.org/10.2139/ssrn.1525612

Bolton, R. J., & Hand, D. J. (2002). Statistical Fraud Detection: A Review. *Statistical Science*, *17*(3), 235-255. https://doi.org/10.1214/ss/1042727940

Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of Fraud Detection Techniques: Credit Card. *International Journal of Computer Applications*, *45*(1), 39-44. https://doi.org/NA

Choi, D., & Lee, K. (2018). An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. *Security and Communication Networks*, *2018*(NA), 5483472-5483415. https://doi.org/10.1155/2018/5483472

Gepp, A., Wilson, J. H., Kumar, K., & Bhattacharya, S. (2021). A Comparative Analysis of Decision Trees Vis-à-vis Other Computational Data Mining Techniques in Automotive Insurance Fraud Detection. *Journal of Data Science*, *10*(3), 537-561. https://doi.org/10.6339/jds.201207_10(3).0010

Gyamfi, N. K., & Abdulai, J.-D. (2018). Bank Fraud Detection Using Support Vector Machine. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, *NA*(NA), NA-NA. https://doi.org/10.1109/iemcon.2018.8614994

Hájek, P., & Henriques, R. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud A comparative study of machine learning methods. *Knowledge-Based Systems*, *128*(128), 139-152. https://doi.org/10.1016/j.knosys.2017.05.001

Hassanzadeh, R. (2014). Anomaly detection in online social networks : using data-mining techniques and fuzzy logic. *NA*, *NA*(NA), NA-NA. https://doi.org/NA

Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decision Support Systems*, *46*(4), 853-864. https://doi.org/10.1016/j.dss.2008.11.013

Hossain, M. A., Islam, S., Rahman, M. M., & Arif, N. U. M. (2024). Impact of Online Payment Systems On Customer Trust and Loyalty In E-Commerce Analyzing Security and Convenience. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 1-15. https://doi.org/10.69593/ajsteme.v4i03.85

Islam, S. (2024). Future Trends In SQL Databases And Big Data Analytics: Impact of Machine Learning and Artificial Intelligence. *International Journal of Science and Engineering*, *1*(04), 47-62. https://doi.org/10.62304/ijse.v1i04.188

Islam, S., & Apu, K. U. (2024). Decentralized Vs. Centralized Database Solutions In Blockchain: Advantages, Challenges, And Use Cases. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *3*(4), 58–68. https://doi.org/10.62304/jieet.v3i04.195

Jim, M. M. I., Hasan, M., Sultana, R., & Rahman, M. M. (2024). Machine Learning Techniques for Automated Query Optimization in Relational Databases. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 514-529.

Kho, J. R. D., & Vea, L. A. (2017). Credit card fraud detection based on transaction behavior. *TENCON 2017 - 2017 IEEE Region 10 Conference*, *NA*(NA), NA-NA. https://doi.org/10.1109/tencon.2017.8228165

Kirlidog, M., & Asuk, C. (2012). A fraud detection approach with data mining in health insurance. *Procedia - Social and Behavioral Sciences*, *62*(NA), 989-994. https://doi.org/10.1016/j.sbspro.2012.09.168

Kowshalya, G., & Nandhini, M. (2018). Predicting Fraudulent Claims in Automobile Insurance. *2018 Second International Conference on Inventive Communication and Computational Technologies*

(ICICCT), *NA*(NA), 1338-1343. https://doi.org/10.1109/icicct.2018.8473034

Liao, S.-H., Chu, P.-h., & Hsiao, P.-Y. (2012). Review: Data mining techniques and applications - A decade review from 2000 to 2011. *Expert Systems with Applications*, *39*(12), 11303-11311. https://doi.org/10.1016/j.eswa.2012.02.063

Ly, M. K.-M. (2014). Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies. *Harvard Journal of Law & Technology*, *27*(2), 587-NA. https://doi.org/NA

Md Abdur, R., Md Majadul Islam, J., Rahman, M. M., & Tariquzzaman, M. (2024). AI-Powered Predictive Analytics for Intellectual Property Risk Management In Supply Chain Operations: A Big Data Approach. *International Journal of Science and Engineering*, *1*(04), 32-46. https://doi.org/10.62304/ijse.v1i04.184

Md Delwar, H., Md Hamidur, R., & Nur Mohammad, A. (2024). Artificial Intelligence and Machine Learning Enhance Robot Decision-Making Adaptability And Learning Capabilities Across Various Domains. *International Journal of Science and Engineering*, *1*(03), 14-27. https://doi.org/10.62304/ijse.v1i3.161

Morshed, A. S. M., Manjur, K. A., Shahjalal, M., & Yahia, A. K. M. (2024). Optimizing Energy Efficiency: A Comprehensive Analysis Of Building Design Parameters. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(04), 54-73. https://doi.org/10.69593/ajsteme.v4i04.120

Mosleuzzaman, M., Shamsuzzaman, H. M., & Hussain, M. D. (2024). Engineering Challenges and Solutions In Smart Grid Integration With Electric Vehicles. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 139-150. https://doi.org/10.69593/ajsteme.v4i03.102

Nandi, A., Emon, M. M. H., Azad, M. A., Shamsuzzaman, H. M., & Md Mahfuzur Rahman, E. (2024). Developing An Extruder Machine Operating System Through PLC Programming with HMI Design to Enhance Machine Output and Overall Equipment Effectiveness (OEE). *International Journal of Science and Engineering*, *1*(03), 1-13. https://doi.org/10.62304/ijse.v1i3.157

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559-569. https://doi.org/10.1016/j.dss.2010.08.006

Omar, N., Johari, Z. A., & Smith, M. (2017). Predicting fraudulent financial reporting using artificial neural network. *Journal of Financial Crime*, *24*(2), 362-387. https://doi.org/10.1108/jfc-11-2015-0061

Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A. (2009). Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning. *Information Fusion*, *10*(4), 354-363. https://doi.org/10.1016/j.inffus.2008.04.001

Peng, H., & You, M. (2016). Trustcom/BigDataSE/ISPA - The Health Care Fraud Detection Using the Pharmacopoeia Spectrum Tree and Neural Network Analytic Contribution Hierarchy Process. *2016 IEEE Trustcom/BigDataSE/ISPA*, *NA*(NA), 2006-2011. https://doi.org/10.1109/trustcom.2016.0306

Rahman, A., Ashrafuzzaman, M., Jim, M. M. I., & Sultana, R. (2024). Cloud Security Posture Management Automating Risk Identification and Response In Cloud Infrastructures. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(03), 151-162. https://doi.org/10.69593/ajsteme.v4i03.103

Rahman, M. M. (2024). Systematic Review of Business Intelligence and Analytics Capabilities in Healthcare Using PRISMA. *International Journal of Health and Medical,*, *1*(4), 34-48. https://doi.org/10.62304/ijhm.v1i04.207

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit Card Fraud Detection Using AdaBoost and Majority Voting. *IEEE Access*, *6*(NA), 14277-14284. https://doi.org/10.1109/access.2018.2806420

Rawte, V., & Anuradha, G. (2015). Fraud detection in health insurance using data mining techniques. *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, *NA*(NA), 1-5. https://doi.org/10.1109/iccict.2015.7045689

Rizki, A. A., Surjandari, I., & Wayasti, R. A. (2017). Data mining application to detect financial fraud in Indonesia's public companies. *2017 3rd International Conference on Science in Information Technology (ICSITech)*, *NA*(NA), 206-211. https://doi.org/10.1109/icsitech.2017.8257111

Rozony, F. Z., Aktar, M. N. A., Ashrafuzzaman, M., & Islam, A. (2024). A Systematic Review Of Big Data Integration Challenges And Solutions For Heterogeneous Data Sources. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(04), 1-18. https://doi.org/10.69593/ajbais.v4i04.111

Sadgali, I., Sael, N., & Benabbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science*, *148*(NA), 45-54. https://doi.org/10.1016/j.procs.2019.01.007

Sah , B. P., Shirin, B., Minhazur Rahman, B., & Shahjalal, M. (2024). The Role of AI In Promoting Sustainability Within the Manufacturing Supply Chain Achieving Lean And Green Objectives. *Academic Journal on Business Administration, Innovation & Sustainability*, *4*(3), 79-93. https://doi.org/10.69593/ajbais.v4i3.97

Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. *Expert Systems with Applications*, *40*(15), 5916-5923. https://doi.org/10.1016/j.eswa.2013.05.021

Saia, R., & Carta, S. (2019). Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks. *Future Generation Computer Systems*, *93*(NA), 18-32. https://doi.org/10.1016/j.future.2018.10.016

Seo, J., & Mendelevitch, O. (2017). EMBC - Identifying frauds and anomalies in Medicare-B dataset. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual International Conference*, *2017*(NA), 3664-3667. https://doi.org/NA

Shahjalal, M., Yahia, A. K. M., Morshed, A. S. M., & Tanha, N. I. (2024). Earthquake-Resistant Building Design: Innovations and Challenges. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *3*(04), 101-119. https://doi.org/10.62304/jieet.v3i04.209

Shamim, M. M. I. (2024). Artificial Intelligence in Project Management: Enhancing Efficiency and Decision-Making. *International Journal of Management Information Systems and Data Science*, *1*(1), 1-6.

Shamim, M. (2022). The Digital Leadership on Project Management in the Emerging Digital Era. *Global Mainstream Journal of Business, Economics, Development & Project Management*, *1*(1), 1-14

Sikder, M. A., Begum, S., Bhuiyan, M. R., Princewill, F. A., & Li, Y. (2024). Effect of Variable Cordless Stick Vacuum Weights on Discomfort in Different Body Parts During Floor Vacuuming Task. *Physical Ergonomics and Human Factors*, *44*.

Supraja, K., & Saritha, S. J. (2017). Robust fuzzy rule based technique to detect frauds in vehicle insurance. *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, *NA*(NA), NA-NA. https://doi.org/10.1109/icecds.2017.8390160

Wu, J., Xiong, H., Wu, P., & Chen, J. (2007). KDD - Local decomposition for rare class analysis. *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, *NA*(NA), 814-823. https://doi.org/10.1145/1281192.1281279

Xiao-yun, W., & Danyue, L. (2010). Hybrid outlier mining algorithm based evaluation of client moral risk in insurance company. *2010 2nd IEEE International Conference on Information Management and Engineering*, *NA*(NA), 585-589. https://doi.org/10.1109/icime.2010.5478070

Yahia, A. K. M., Rahman, D. M. M., Shahjalal, M., & Morshed, A. S. M. (2024). Sustainable Materials Selection in Building Design And Construction. *International Journal of Science and Engineering*, *1*(04), 106-119. https://doi.org/10.62304/ijse.v1i04.199

Zareapoor, M., & Shamsolmoali, P. (2015). Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. *Procedia Computer Science*, *48*(48), 679-685. https://doi.org/10.1016/j.procs.2015.04.201

Zhang, D., & Zhou, L. (2004). Discovering golden nuggets: data mining in financial application. *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, *34*(4), 513-522. https://doi.org/10.1109/tsmcc.2004.829279